Отзыв научного руководителя о диссертации Кнопа Александра Анатольевича

«Сложность эвристических вычислений и интерактивных протоколов»,

представленной на соискание ученой степени кандидата физико-математических наук по специальности 01.01.06 — математическая логика, алгебра и теория чисел.

Диссертация А. А. Кнопа относится к математической логике, а именно, к теории сложности вычислений. В ней исследуются свойства эвристических вычислений и вычислений с ограничением на время работы в среднем. В диссертации доказываются оценки на эвристическую схемную сложность языков, распознаваемых эвристическими протоколами Мерлин–Артур, доказываются теоремы об иерархии по времени для ряда классов эвристических вычислений и доказываются теоремы об иерархии распределенных задач относительно сложности распределения. Это важная и популярная в последнее время тематика; результаты о нижних оценках всегда представляют особенный интерес; теоремы об иерархии являются классическим способом изучения структуры сложностных классов.

Наличие в постановке задачи не только языка (множества входов, для которых ответ в задаче положителен), но и вероятностного распределения на входах имеет как практическую алгоритмическую мотивацию (когда важна сложность не в наихудшем случае, а для "наиболее частых", "типичных" данных), так и криптографическую (важно защититься от взлома не в наихудшем для взломщика случае, а в любой ситуации, случающейся с заметной вероятностью). Известно, что функции, сложные для обращения в среднем, существуют тогда и только тогда, когда существуют криптографические односторонние функции. Для таких пар из языка и распределения естественным образом формулируются два вида сложности: эвристическая (когда алгоритм может быть некорректен на некоторой небольшой относительно данного распределения доле входов) и в среднем (когда алгоритм должен быть корректен на каждом входе, но время его работы оценивается в среднем — по техническим соображениям речь идёт не о математическом ожидании, а о чуть более сложном определении).

Оказывается, что в такой постановке имеют решение некоторые вопросы, считающиеся "неподъёмными" в классической теории сложности. В диссертации А. А. Кнопа изучаются два таких типа вопросов: в каком наименьшем классе можно найти функции произвольной полиномиальной сложности, и для каких классов можно построить (строгие) иерархии по времени (т.е. показать, что есть задачи, которые можно решить за большее время, но нельзя за меньшее).

В уменьшении классов, для которых можно доказать нижние оценки, прогресс остановился чуть ниже второго уровня полиномиальной иерархии. Для второго уровня — это классический результат Каннана, а максимум, куда удалось спуститься — симметричная версия второго уровня (результат Кая). Протоколы Мерлина и Артура являются обобщением классического класса **NP**, только проверка доказательства является вероятностной. Для них нелинейные нижние оценки схемной сложности по-прежнему не доказаны. Сантанаму удалось доказать такие оценки лишь в случае, когда участники получают один бит непроверяемой (неравномерной) подсказки, т.е. для алгоритмически неразрешимых задач. А. А. Кноп в первой